Catalogue no. 85-002-X
ISSN 1209-6393

Juristat

Police-reported cybercrime in Canada, 2012

by Benjamin Mazowita and Mireille Vézina

Release date: September 25, 2014

Statistics Canada Statistique Canada

Canada

How to obtain more information

For information about this product or the wide range of services and data available from Statistics Canada, visit our website, www.statcan.gc.ca.

You can also contact us by

email at infostats@statcan.gc.ca,

telephone, from Monday to Friday, 8:30 a.m. to 4:30 p.m., at the following toll-free numbers:

• Statistical Information Service	1-800-263-1136
• National telecommunications device for the hearing impaired	1-800-363-7629
• Fax line	1-877-287-4369

Depository Services Program

• Inquiries line	1-800-635-7943
• Fax line	1-800-565-7757

To access this product

This product, Catalogue no. 85-002-X, is available free in electronic format. To obtain a single issue, visit our website, www.statcan.gc.ca, and browse by "Key resource" > "Publications."

Standards of service to the public

Statistics Canada is committed to serving its clients in a prompt, reliable and courteous manner. To this end, Statistics Canada has developed standards of service that its employees observe. To obtain a copy of these service standards, please contact Statistics Canada toll-free at 1-800-263-1136. The service standards are also published on www.statcan.gc.ca under "About us" > "The agency" > "Providing services to Canadians."

Published by authority of the Minister responsible for Statistics Canada

Cette publication est aussi disponible en français.

Note of appreciation

Canada owes the success of its statistical system to a long-standing partnership between Statistics Canada, the citizens of Canada, its businesses, governments and other institutions. Accurate and timely statistical information could not be produced without their continued co-operation and goodwill.

Standard symbols

The following symbols are used in Statistics Canada publications:

.	not available for any reference period
..	not available for a specific reference period
...	not applicable
0	true zero or a value rounded to zero
0^s	value rounded to 0 (zero) where there is a meaningful distinction between true zero and the value that was rounded
p	preliminary
r	revised
x	suppressed to meet the confidentiality requirements of the *Statistics Act*
E	use with caution
F	too unreliable to be published
*	significantly different from reference category ($p < 0.05$)

Police-reported cybercrime in Canada, 2012: highlights

- In 2012, 9,084 incidents of cybercrime were reported by select police services policing 80% of the population of Canada. This represented a rate of 33 cybercrime incidents per 100,000 population.
- The most common type of cybercrime was fraud, accounting for more than half (54%) of all police-reported cybercrimes in 2012. Intimidation violations, composed of violations involving the threat of violence, accounted for 20% of police-reported cybercrimes in 2012, while 16% of cybercrimes involved a sexual cyber-related violation.
- In 2012, an accused was identified by police in a relatively small proportion (6%) of cybercrimes against property, notably for incidents of fraud (5%) and identity theft (3%).
- An accused was identified by police in connection with 31% of sexual cyber-related violations and 55% of cybercrimes related to intimidation violations. Compared to intimidation violations, sexual violations were more frequently cleared by the laying of a charge (25% versus 18%).
- The majority (76%) of accused identified by police in 2012 were men. For cyber-related violations of a sexual nature, males accounted for 94% of accused.
- Accused identified by police in connection with intimidation violations tended to young, with more than one-quarter (28%) under the age of 18, whereas those accused of cybercrimes of a sexual nature tended to be somewhat older, as the largest proportion (22%) of accused of sexual cybercrimes were aged 25 to 34.
- In 2012, police identified 2,070 victims of violent incidents involving a cybercrime. Females accounted for the majority of victims of violent incidents associated with a cybercrime (69%), particularly when incidents involved a sexual violation (84%).
- Overall, 42% of victims of police-reported cybercrime were under the age of 18. In 2012, almost all (96%) victims of sexual violations associated with a cybercrime were under 18 years of age, including 10% of victims under the age of 12.
- Most victims (73%) of violent incidents associated with a cybercrime knew the accused. Victims of sexual violations involving a cybercrime were less likely to know the accused (57%) relative to victims of non-sexual violent violations (77%).
- According to results from the 2009 General Social Survey on Victimization, approximately 1.75 million Canadians aged 15 and over reported that they had been cyber-bullied. This represented 8% of Internet users aged 15 and over. Less than one in ten (7%) victims of cyber-bullying reported the incident to police.

Police-reported cybercrime in Canada, 2012

by Benjamin Mazowita and Mireille Vézina

The Internet is an increasingly integral part of the daily lives of Canadians. According to results from the Canadian Internet Use Survey, 83% of Canadians aged 16 and over accessed the Internet for personal use in 2012. A majority of Internet users in Canada did their banking online (72%), visited social networking sites (67%), and ordered goods and services online (56%). The total dollar value of orders placed online by Canadians reached $18.9 billion in 2012 (Statistics Canada 2013).

The rapid growth in Internet use has allowed for the emergence of new criminal opportunities (Nuth 2008). Criminal offences involving a computer or the Internet as either the target of a crime or as an instrument used to commit a crime are collectively known as cybercrime (see Text box 1). Frauds, identity theft, extortion, criminal harassment, certain sexual offences, and offences related to child pornography are among the criminal violations that can be committed over the Internet using a computer, tablet, or smart phone.

Using data from the 2012 Incident-based Uniform Crime Reporting Survey (UCR2.2), this *Juristat* article examines police-reported cybercrime in Canada[1,2] Analysis is presented on the number of cybercrimes reported by police services covering 80% of the population of Canada, as well as the characteristics of incidents, victims, and persons accused of cyber-related violations. These findings are supplemented with self-reported data on cyber-bullying, based on results from the 2009 General Social Survey (GSS) on Victimization.

Police-reported cybercrime

Text box 1
Defining and measuring police-reported cybercrime

Definition

Cybercrime is a complex phenomena and its non-traditional characteristics pose various challenges for police services and the criminal justice system as a whole. The lack of reliable information on cybercrime has been identified as a significant impediment to the development of crime prevention strategies addressing cybercrime (Smyth and Carleton 2011).

The collection of reliable cybercrime statistics requires a standardized definition. The Uniform Crime Reporting Survey has adopted the definition of cybercrime developed by the Canadian Police College: "a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence" (Kowalski 2002). Cybercrimes can thus be divided into two broad categories: incidents in which computers or the Internet are the **target** of a crime, such as computer hacking and unauthorized use of computer systems, and incidents in which computers or the Internet are the **instrument** used to commit a crime, such as luring a child via a computer or fraud perpetrated over the Internet (Canadian Centre for Justice Statistics 2013). In 2012, police indicated that in 88% of reported cybercrimes a computer or the Internet was used as the instrument to commit an offence, while in 10% of reported cybercrimes a computer or the Internet was the target of the offence. The cybercrime type could not be determined for the remaining 2% of incidents.

Text box 1 continued
Defining and measuring police-reported cybercrime

Incident based data

Police services covering 80% of the population of Canada reported cybercrime data to the Canadian Centre for Justice Statistics (CCJS) in 2012 through the UCR2.2 Incident-based Survey.[3] A criminal incident may be comprised of multiple violations of the law. When reporting data to the Uniform Crime Reporting Survey, police can include up to four violations in an incident. To ensure consistent reporting over time and across police services, police-reported criminal incidents are counted according to the '**most serious violation**' in the incident. However, for the purposes of analyzing incidents of cybercrime, one distinct violation within the incident was identified as the '**cyber-related violation**.' The cyber-related violation represents the specific criminal violation within an incident in which a computer or the Internet was the target of the crime or the instrument used to commit the crime. While in the majority (99%) of incidents of cybercrime the cyber-related violation is the most serious violation in the incident, there are a small number of cybercrime incidents where this is not the case. For example, in an incident involving both the sending of threatening e-mails and a physical assault, the cyber-related violation would be uttering threats while the most serious violation within the incident would be assault. See Text box 3 for more information on incidents of cybercrime where the cyber-related violation is not the most serious violation within the incident.

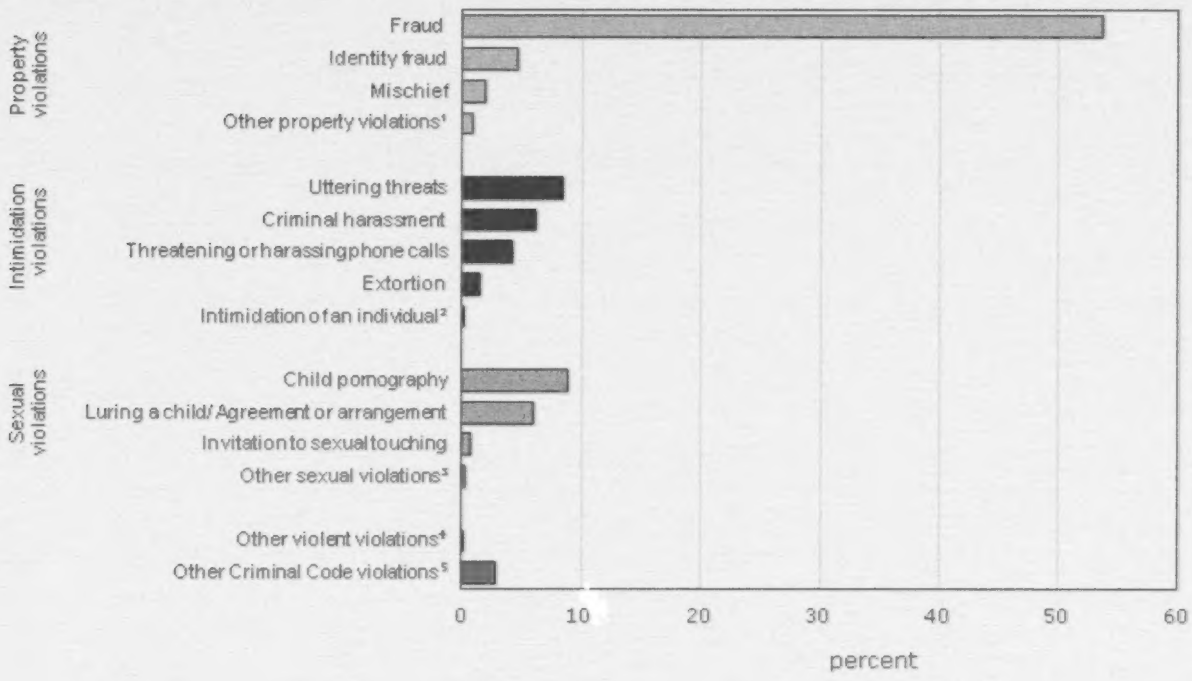
For the purposes of the present analysis, findings related to the characteristics of cybercrime incidents and those accused of cybercrime are presented according to the **cyber-related violation**. In contrast, analysis of victims of cybercrime is presented according to the **violation against the victim**, in order to identify the most serious violation committed against individual victims.

Frauds account for more than half of all police-reported cybercrime incidents

In 2012, 9,084 incidents of cybercrime were reported by police services covering 80% of the population of Canada. This represented a rate of 33 cybercrime incidents per 100,000 population[4] (Table 1).

Offences against property accounted for the majority (61%) of cybercrime incidents in 2012, amounting to 5,544 incidents. Fraud[5] alone accounted for more than half (54%) of all cybercrimes substantiated by police. Other notable property-related cybercrimes included identity fraud (5%), mischief (2%), and identity theft (1%).[6]

Chart 1
Police-reported cybercrime, by violation type, selected police services, 2012



1. Other property violations include identity theft and trafficking stolen goods.
2. Intimidation of an individual includes intimidation of a justice system participant or journalist and intimidation of a non-justice system participant.
3. Other sexual violations include voyeurism, sexual exploitation, corrupting children, making sexually explicit material available to children, and bestiality - commit or compel person.
4. Other violent violations include trafficking in persons and other violent violations.
5. Other *Criminal Code* violations include offences such as corrupting morals, indecent acts, offences against the person and reputation, fail to comply with order, and breach of probation.

Note: This chart reflects data reported by police services covering 80% of the population of Canada.
Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey

In 2012, police reported 3,284 criminal incidents where the cyber-related violation was a violation against the person[7], representing 36% of all reported cybercrimes. For the purposes of this analysis, cybercrimes against the person have been split into two distinct categories: **intimidation violations**, composed of violations involving the threat of violence, such as uttering threats, criminal harassment, and extortion, and **sexual violations**, including violations such as luring a child via a computer and child pornography offences. For a complete list of which violations are included within the respective categories, see Table 1.

Intimidation violations accounted for one in five (20%) police-reported cybercrimes in 2012, amounting to 1,839 incidents. Uttering threats and criminal harassment, accounting for 8% and 6% of reported cybercrimes respectively, were the most common intimidation violations.

In 2012, police reported 1,441 incidents of cybercrime where the cyber-related violation was a sexual violation, representing 16% of all police-reported cybercrimes. Luring a child via a computer[8] accounted for a significant proportion of sexual cyber-related violations, equating to 6% of all police-reported cybercrimes. An additional 9% of police-reported cybercrimes consisted of child pornography offences[9], which include accessing, possessing, producing, and distributing child pornography. In 2012, there were 805 incidents of cybercrime investigated by select Canadian police services where the cyber-related violation was a child pornography offence.

An additional 3% of cybercrime incidents were other *Criminal Code* violations, including offences such as corrupting morals, indecent acts, and offences against the person and reputation.

Text box 2
Cybercrimes coming to the attention of police

The reporting of cybercrimes to the police can be influenced by a variety of factors. As with police-reported crime more generally, the reporting and collection of statistics may be influenced by local police services' procedures, public perceptions and willingness to report victimizations to police, and various legislative and social factors (Brennan 2012).

The detection of cybercrime by police can be influenced by the amount of resources local police services have in the field. For example, the existence of a dedicated cybercrime unit within a police service will impact a police service's capacity to detect and investigate cybercrimes. As such, the data may, in part, reflect differences in resources and strategies of police services in detecting cybercrime.

Police have indicated that advances in technology, including the proliferation of smart phones, anonymous online networks, virtual currency schemes, and cloud computing, have created new opportunities for criminals and require innovative policing measures (RCMP 2014).

Further, the irregular spatial characteristics of cybercrime pose unique obstacles in terms of the identification and investigation of cybercrime incidents. Unlike most conventional crimes, many cybercrimes cannot be anchored to precise geographic boundaries. Cybercrimes may be committed remotely and in decentralized virtual networks, crossing provincial and national boundaries. Police-reported data indicates the jurisdiction where the offence was reported and recorded but not necessarily where the incident or victimization occurred. The laws, resources, and activities devoted to cybercrime may vary from one jurisdiction to the next and over time, influencing the amount of cybercrime coming to the attention of police. Given the unique nature of cybercrime, any comparisons over time or between jurisdictions are not recommended.

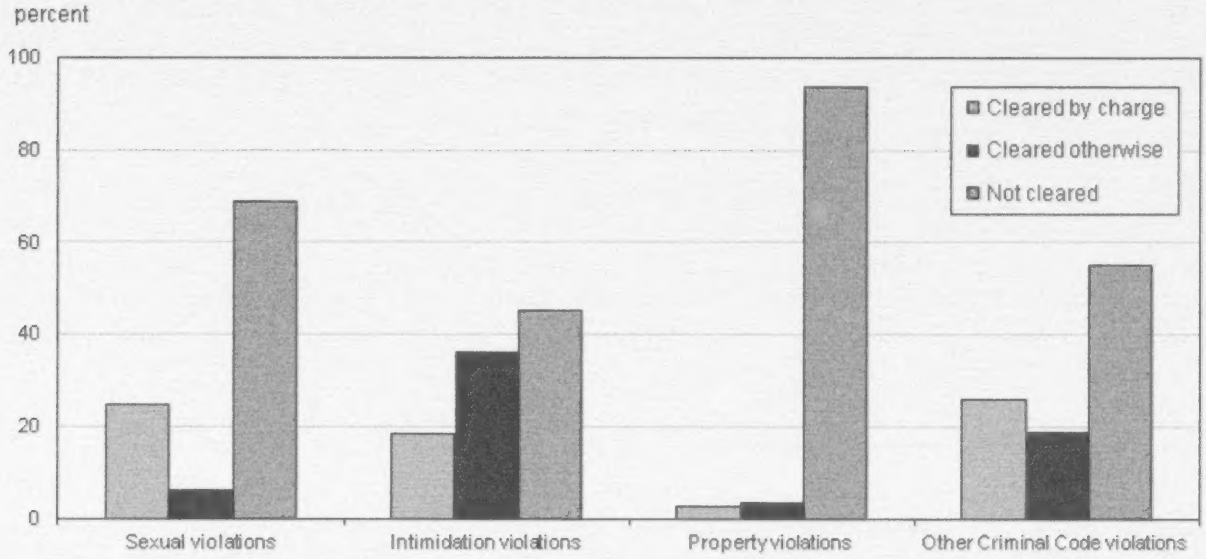
An accused is more likely to be identified in incidents of cybercrime against the person

An accused was identified in 21% of police-reported cybercrime incidents in 2012, meaning the remaining 79% of cybercrime incidents coming to the attention of police that year were not cleared[10] (Table 2).

In 2012, 6% of property-related cybercrimes were cleared by a charge or cleared otherwise. The low clearance rate of property-related cybercrimes was the result of an accused being identified in only a small proportion of incidents of fraud (5%) and identity theft (3%).

In contrast, 31% of sexual cyber-related violations and 55% of cybercrimes related to intimidation violations were cleared by a charge or cleared otherwise in 2012 (Chart 2). The clearance rate of sexual cybercrimes was impacted by an accused only being identified in 23% of incidents of child pornography, the most common sexual cyber-related violation.

Chart 2
Police-reported cybercrime, by violation type and clearance status, selected police services, 2012



Note: This chart reflects data reported by police services covering 80% of the population of Canada. For an incident to be cleared, an accused must be identified and there must be enough evidence to lay a charge in connection with the incident. Incidents may be cleared by charge or processed by other means (i.e. cleared otherwise). Sexual violations include sexual violations against the person and child pornography related offences. Intimidation violations include violations against the person involving the threat of violence. The category Property violations includes fraud, identity theft, identity fraud, mischief and trafficking stolen goods. The category Other *Criminal Code* violations includes offences such as corrupting morals, indecent acts, and offences against the person and reputation. A small number of incidents categorized as other violent violations are excluded from this chart. See Table 1 for a list of offences in each violation type category.
Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

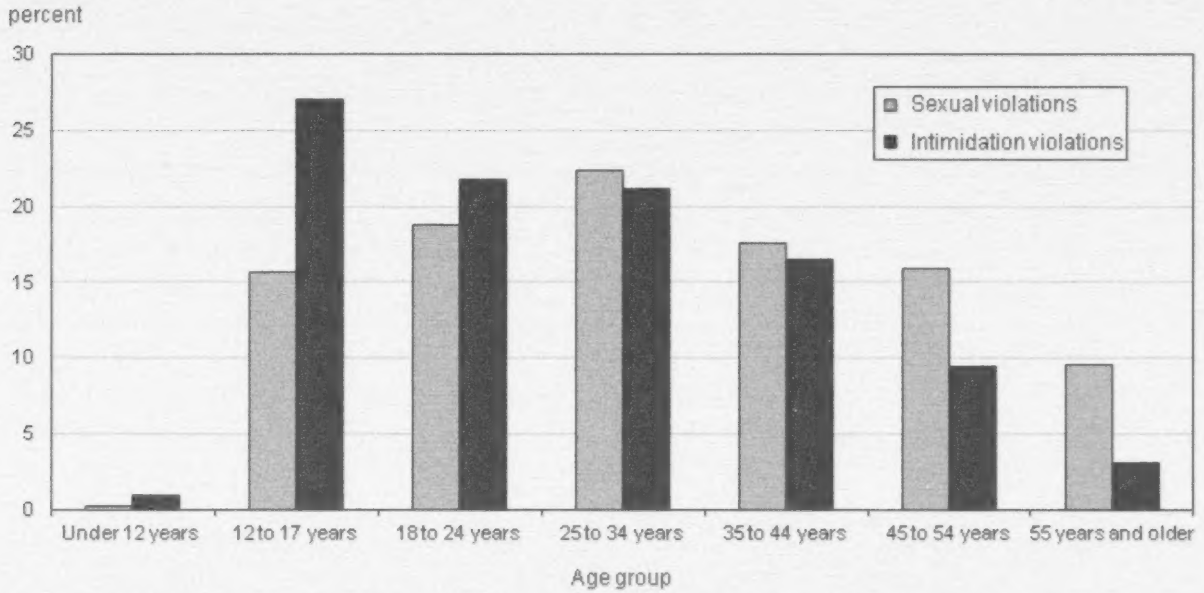
Compared to intimidation violations, sexual cybercrimes were more frequently cleared by the laying of a charge (25% versus 18%). This was the result of numerous intimidation violations, particularly uttering threats and criminal harassment, being cleared by means other than the laying of a charge. For these violations, accused were often not charged at the discretion of the police service or in cases where the complainant declined to lay charges for the incident.

The majority of accused of police-reported cybercrimes are men

In 2012, police identified 2,051 individuals accused of cybercrime incidents (Table 3). The majority (76%) of these accused were men, with adult men between the ages of 18 and 34 accounting for 37% of all persons accused of a police-reported cybercrime that year. The tendency for those accused of cybercrimes to be male was especially pronounced for violations of a sexual nature, where males accounted for 94% of accused identified by police.

Accused identified by police in connection with intimidation violations tended to young, whereas those accused of cybercrimes of a sexual nature tended to be somewhat older (Chart 3). More than one-quarter (28%) of those accused of intimidation violations were under the age of 18, with the proportion of accused declining with increasing age. In contrast, the largest proportion (22%) of accused of sexual cybercrimes were aged 25 to 34, and 16% of accused identified in connection with incidents of child pornography, the most common sexual cyber-related violation, were aged 55 years or older.

Chart 3
Age distribution of persons accused of a cyber-related violation against the person, by sexual violations and intimidation violations, selected police services, 2012



Note: This chart reflects data reported by police services covering 80% of the population of Canada. Accused counts are based upon the cyber-related violation within the incident. Sexual violations include sexual violations against the person and child pornography related offences. Intimidation violations include violations against the person involving the threat of violence. Accused records with unknown age or sex are excluded. See Table 1 for a list of offences in each violation type category.
Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

Those accused of cybercrimes against property were more likely to be aged 18 years or older, with adult males and adult females accounting for 67% and 24% of accused respectively. Approximately four in ten (41%) accused identified by police in connection with a property-related cybercrime were between the ages of 25 and 34.

Text box 3
A small number of police-reported cybercrimes are committed in conjunction with a more serious violation

A criminal incident may be comprised of multiple violations of the law. When reporting data to the Uniform Crime Reporting Survey, police can include up to four violations in an incident. Generally, where an incident is composed of multiple criminal violations, it is categorized by the most serious violation in the incident according to standard survey rules. However, for the purposes of analyzing cybercrime data, one violation within the incident was determined to be the cyber-related violation. The most serious violation and the cyber-related violation are not necessarily the same. While the analysis of incidents in this *Juristat* is based on the cyber-related violation, this text box provides some insight into those incidents that also comprised a more serious violation.

In 2012, the cyber-related violation and the most serious violation in the incident were the same for almost all cybercrime incidents (99%). The remaining 1% represented 110 incidents of cybercrime where the cyber-related violation was not the most serious violation in the incident.

In 2012, there were 71 incidents of cybercrime (involving 87 victims) where there was also a sexual assault or sexual interference offence in the incident and 26 incidents (involving 30 victims) that involved a physical assault.

The presence of a more serious violent offence within an incident was notable for several types of cyber-related violations. In 2012, 20 of the 67 incidents where the cyber-related violation was invitation to sexual touching also included the more serious violation of sexual assault or sexual interference within the incident. Similarly, of the 543 incidents where the cyber-related violation was luring a child via a computer, 33 of those incidents also involved the more serious violations of sexual assault or sexual interference.

Text box 3 continued

A small number of police-reported cybercrimes are committed in conjunction with a more serious violation

For cybercrimes related to intimidation violations, 17 of the 759 incidents of uttering threats and 12 of the 560 incidents of criminal harassment involved a more serious violent violation within the incident, including sexual assault, physical assault, and forcible confinement.

An accused was more likely to be identified in cybercrime incidents that were associated with a more serious violation. In 2012, 82% of cybercrime incidents that involved a more serious violation than the cyber-related violation were cleared by charge, while 8% were cleared otherwise. Incidents of cybercrime that included a more serious violent violation within the incident, such as sexual assault or physical assault, were also more likely to involve an accused who was known to the victim. Victims of sexual assaults or sexual interference associated with a cybercrime were most commonly victimized by a friend or acquaintance (56%), whereas victims of physical assaults associated with a cybercrime were most commonly victimized by a current or former intimate partner (55%).

A majority of identified victims of violent incidents involving cybercrime are female

In 2012, police identified 2,070 victims of violent incidents involving a cyber-related violation[11] (Table 4). This includes 468 victims of sexual violations and 1,602 victims of non-sexual violent violations.[12]

Just over two-thirds (69%) of victims associated with incidents of cybercrime were female. Females accounted for 84% of victims of sexual violations associated with a cybercrime and 65% of those involving non-sexual violent violations.

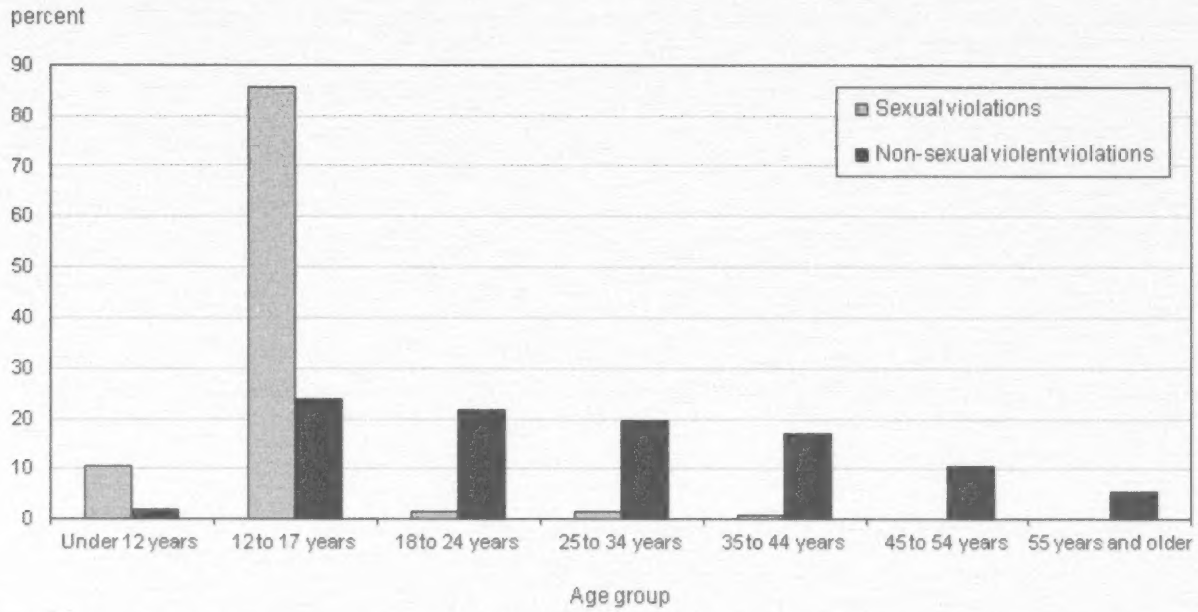
Victims of violent incidents involving a cybercrime tend to be young

Victims of police-reported cybercrime are generally young. Overall, 42% of victims of cybercrime identified by police were aged 17 and under, while an additional 17% of victims were aged 18 to 24.

The prevalence of victims under the age of 18 was especially pronounced for violations of a sexual nature (Chart 4). In 2012, 96% of these victims were aged 17 and under, including 10% of victims under the age of 12. Common sexual cyber-related violations, notably invitation to sexual touching, and luring a child via computer, are sexual violations that expressly target child victims.

Previous analysis of police-reported crime in Canada has found that youth account for a disproportionate number of victims of sexual offences. In 2012, children and youth accounted for 55% of victims of all police-reported sexual offences while only accounting for 20% of the population of Canada (Cotter and Beaupré 2014).

Chart 4
Age distribution of victims of violent violations associated with a cybercrime, by sexual violations and non-sexual violent violations, selected police services, 2012



Note: This chart reflects data reported by police services covering 80% of the population of Canada. Victim counts are based on the violation against the victim. Sexual violations include sexual violations against the person for which victim information is collected. Non-sexual violent violations include assaults, violations involving the threat of violence, and other violent violations. Victim records with unknown age or sex are excluded. See Table 5 for a list of offences in each violation type category.
Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

Relative to violent sexual offences, victims of non-sexual violent violations associated with a cybercrime tended to be somewhat older. Approximately one quarter (26%) of victims were aged 17 or under, while the remaining 74% were aged 18 years or older.

Victims of violent violations associated with a cybercrime generally know the accused

Almost three-quarters (73%) of victims of violent violations associated with a police-reported cybercrime knew the accused (Table 5). In a majority of incidents, the accused was known to the victim as a friend or acquaintance (45%), a current or former intimate partner (24%), or a family member (5%). For just over one-quarter (27%) of victims the accused was not known to the victim.[13]

Relative to non-sexual violent violations, victims of sexual violations associated with a cybercrime were less likely to know the accused. About six in ten (57%) victims of sexual violations knew the accused, most commonly as a friend or acquaintance (45%). The remaining 43% of victims of sexual violations associated with a cybercrime did not know the accused. The accused was a stranger for the majority (55%) of victims of luring a child via a computer, the most common violent sexual violation associated with cybercrimes.

For incidents of cybercrime involving a non-sexual violent violation, the accused was most likely to be a friend or acquaintance (44%) or a current or former intimate partner (28%). More specifically, victims of criminal harassment had the highest proportion of accused who were identified as a current or former intimate partner (47%), most commonly a former dating partner (32%). Victims of threatening or harassing phone calls were most likely to have been victimized by a friend or acquaintance (44%), while more than half of victims of extortion did not know the accused (60%).

Text box 4
Alternate data sources

Police-reported cybercrime data represent cybercrimes coming to the attention of police and thus are an underestimation of Internet victimization experienced by Canadians. For example, while constituting a significant proportion of police-reported cybercrime, many occurrences of online fraud and identity theft are not reported or do not come to the attention of police (Smyth and Carleton 2011). According to results from the 2009 General Social Survey on Victimization, 4% of Internet users were the victim of bank fraud during the 12 months preceding the survey (Perreault 2011).

Aside from policing and victimization data, several private organizations and public agencies collect and report data on the incidence of cybercrime in Canada. The types of data collected and the methods used vary according to the mandate of the respective agencies and the field in which they operate. In some cases, the information comes directly from what the public reports, while in other cases, the data are collected by surveys of Canadians on their experiences with cybercrime.

In 2013, **Norton** published a research study commissioned by Symantec on the prevalence and financial costs of cybercrime, based on a survey of adult Internet users across 24 countries. The study estimated that 68% of Canadian adult Internet users had experienced cybercrime in their lifetime, while 42% had experienced cybercrime in the 12 months preceding the survey. Additionally, the study estimated that the cost of cybercrime in Canada in the 12 months preceding the survey was approximately $3 billion US dollars (Norton 2013). These findings are corroborated by research conducted by the **Center for Strategic and International Studies** sponsored by Intel Security. According to the research, based on public data and input from government officials, experts, and cybersecurity companies, the annual cost of cybercrime in Canada equated to 0.17% of Canada's Gross Domestic Product (Center for Strategic and International Studies 2014).

Targeting the different types of mass marketing (telemarketing) fraud such as spam and identity fraud, the **Canadian Anti-Fraud Centre** collects data based on complaints and calls from victims. These complaints are received by telephone at a national call centre. Formerly known as Phonebusters, this initiative is carried out in collaboration with the RCMP, the Canadian Competition Bureau, and the Ontario Provincial Police, and it reports on the number of complaints received according to the mode of solicitation, such as by the Internet, by telephone or by mail. In 2013 the Canadian Anti-Fraud Centre received approximately 43,000 complaints of mass marketing fraud, representing approximately 12,000 victims with a total reported dollar loss in excess of $52 million dollars. According to the data, e-mail or the Internet were the methods of solicitation accounting for 56% of total reported dollar loss. Additionally, the Canadian Anti-Fraud Centre identified almost 20,000 victims of identity fraud in 2013, with a total reported dollar loss of approximately $11 million dollars (Canadian Anti-Fraud Centre 2014).

Cybertip.ca, which is operated by a charitable organization called the Canadian Centre for Child Protection, receives and analyzes information on the sexual exploitation of children on the Internet. This information comes from tips supplied by the public online and by telephone in connection with offences such as child pornography, child luring and child trafficking. In 2013/2014, there were 24,911 reports to Cybertip.ca concerning the online sexual exploitation of children. Those tips were analyzed and then sent to the appropriate police agency or child protection agency when there was reason to believe that a criminal incident had occurred (Cybertip.ca 2014).

Self-reported cyber-bullying

As with crime in general, one of the limitations of police-reported cybercrime data is that not all cybercrimes come to the attention of police. In 2009, the General Social Survey (GSS) collected information on persons who reported having been victimized on the Internet, irrespective of whether or not the victimization came to the attention of police. These data complement police-based data in estimating the prevalence of Internet victimization in Canada.[14]

Using results from the 2009 GSS on Victimization, the following section takes a closer look at the characteristics of self-reported victims of cyber-bullying, as well as the protective measures and precautions that those who have experienced cyber-bullying have taken in their daily lives (see Text box 5).

Text box 5
Defining self-reported victimization on the Internet

The following definitions are derived from the questions asked to Canadians aged 15 and over in the 2009 General Social Survey (GSS). It is important to note that data obtained from these questions are based on people's perceptions and should not be compared with police-reported data.

Cyber-bullying: The GSS asked Canadians if they had ever previously received threatening or aggressive messages; been the target of hate comments spread through e-mails, instant messages, or postings on Internet sites; or threatening e-mails using the victim's identity.

Protective measures: In the GSS, persons aged 15 and over were asked whether they had taken one or more of the following steps to protect their safety or their property against criminal acts during the 12 months preceding the survey: changed their routine or activities or avoided certain people or places; installed new locks or security bars; installed motion detector lights; taken a self-defence course; obtained a dog; obtained a firearm; and changed residence or moved.

Precautions in daily life: The GSS also asked Canadians about the precautions that they were taking in their daily lives. Unlike protective measures, precautions taken do not have a specific reference period. These can be new habits, adopted in the last few months, or habits formed many years ago. The precautions are the following: carry something to defend yourself or alert other people; when alone and returning to a parked car, check the back seat for intruders before getting into the car; plan your route with safety in mind; stay at home at night because you are afraid to go out alone; lock windows and doors at home; rather than walk, use your car, a taxi or public transportation for your personal safety.

Internet users: For the purposes of this article, Internet users are those who reported using the Internet in the 12 months prior to the survey.

Adolescents were the most likely to report being the target of cyber-bullying

In 2009, approximately 1.75 million Canadians aged 15 and over reported that they had been cyber-bullied. This represented 8% of Internet users aged 15 and over. Nearly one in five (19%) youth[15] aged 15 to 17 reported they had been a victim of cyber-bullying, while this was the case for 17% of young adults aged 18 to 24. The proportion fell to 9% for the 25-34 age group and subsequently to 5% or less for age groupings 35 and over (Table 6).

Users of social networking sites were more likely to report being cyber-bullied

Social networking sites such as Facebook and MySpace are major platforms for social exchanges. The use of such social networking platforms is also associated with an elevated risk of being the target of cyber-bullying. In 2009, according to GSS data, 12% of users of social networking sites aged 15 and over reported being a victim of cyber-bullying, while this was the case for 3% of those not engaged in social networking. Among users of online chat rooms, 15% reported having been a victim of cyber-bullying, more than twice the proportion of those who did not use these forums (5%).

While the use of social networking sites is especially prevalent among young people, users of social networking sites were consistently at a greater risk of experiencing cyber-bullying regardless of age. In effect, 19% of users of social networking sites between the ages of 18 and 24 reported having been a victim of cyber-bullying, compared to 9% of those who did not engage in social networking. Among those aged 45 to 54, 8% of users of social networking sites reported being cyber-bullied, compared to 3% among those who did not use these websites.

One in five victims of cyber-bullying also reported being the target of a violent crime

Results from the 2009 GSS indicate that online victimization was associated with an increased incidence of violent victimization. In 2009, 11% of Internet users aged 15 and over who reported being cyber-bullied also reported receiving threats of a physical attack and 21% reported being the victim of at least one violent crime in the 12 months preceding the survey. By comparison, among non-victims of cyber-bullying, 6% reported being the victim of at least one violent crime. This difference was especially pronounced among youth. The proportion of victims of cyber-bullying aged 15 to 17 who were also the victim of a violent crime was 32%. In comparison, this was the case for 12% of respondents in this age group who did not report having experienced cyber-bullying. Among those aged 18 to 24, 27% of victims of cyber-bullying also reported being the victim of a violent crime, relative to 12% of those who did not report having been cyber-bullied.

The findings of the GSS do not indicate if those accused of committing violent crimes are those who engage in acts of cyber-bullying. Further research is required to examine the relationship between Internet victimization and violent victimization.

The majority of victims of cyber-bullying did not report the incident to the police

Less than one in ten (7%) victims of cyber-bullying reported the incident to police according to 2009 GSS data. The incident was reported to police by 8% of female victims of cyber-bullying and 5% of male victims of cyber-bullying. Research has found that younger age groups are less likely to report incidents of victimization to police (Perreault and Brennan 2010).

Previous research has found that victims of cyber-bullying are more likely to block messages from the sender, leave the Internet site, or report the situation to their Internet service provider than to report the incident to the police (Perreault 2011).

More than half of victims of cyber-bullying reported taking protective measures

The 2009 GSS asked survey respondents if they had taken certain protective measures for their personal safety in the 12 months preceding the survey. In all, 59% of persons who were victims of cyber-bullying said that they had taken at least one protective measure (Table 7). The percentage was 40% for non-victims of cyber-bullying.[16]

Among persons who reported being a victim of both cyber-bullying and a violent crime, three in four (75%) had taken a protective measure, compared with 54% of Canadians who were victims of cyber-bullying only. For persons who had not been victims of cyber-bullying or a violent crime, this proportion was 39%.

Among the protective measures taken, 47% of all victims of cyber-bullying stated that they had changed their routine or activities, or avoided certain people or places, while 18% reported having installed new locks or security bars. Among non-victims of cyber-bullying, the corresponding percentages were 28% and 13% respectively.

Victims of cyber-bullying reported taking more daily precautions

In addition to new protective measures discussed in the preceding section, the GSS on Victimization also questioned Canadians about certain precautions that could be taken in daily life.[17] Victims of cyber-bullying reported that they were more inclined than non-victims of cyber-bullying to take certain precautions. Among cyber-bullying victims, 28% carried something to defend themselves, compared with 15% of non-victims of cyber-bullying (Table 7). More than half (53%) of cyber-bullying victims planned their route with safety in mind, compared with 43% of non-victims of cyber-bullying. Among victims, 14% said they stayed at home because they were afraid, compared with 8% of those who did not experience cyber-bullying.

Victims of cyber-bullying who also reported being victims of at least one violent crime were more likely than those who were not victims of a violent crime to take more precautions. Among cyber-bullying victims who were also victims of violent crime, 47% had taken at least four precautions, compared with 32% of persons who reported being victims of Internet bullying only.

In general, women were more likely than men to take daily precautions. According to GSS data, 49% of female victims of online bullying said they took at least four precautions, 12 percentage points higher than for females who were not victims of cyber-bullying (37%). For men, 20% of victims of cyber-bullying reported taking at least four safety precautions, compared with 11% of males who were not victims of cyber-bullying.

Victims of cyber-bullying report higher stress levels than non-victims

Victims of cyber-bullying were more likely to report higher levels of stress in their daily lives than non-victims. In 2009, more than one-third (36%) of victims reported that their days were quite a bit stressful or extremely stressful, compared with 24% of those who were not victims of cyber-bullying.

In general, females were more likely than males to report higher levels of stress. Regardless of their gender, cyber-bullying victims were more likely to report that their days were quite a bit or extremely stressful. This was the case for 39% of female victims, compared with 26% of non-victims. Among male victims of cyber-bullying, 32% reported that their days were quite a bit or extremely stressful, while the proportion was 23% for non-victims.

Summary

In 2012, police services covering 80% of the Canadian population reported 9,084 incidents of cybercrime. The most common type of cybercrime was fraud, accounting for more than half (54%) of all police-reported cybercrimes in 2012. Intimidation violations, composed of violations involving the threat of violence, accounted for 20% of police-reported cybercrimes in 2012, while 16% of cybercrimes involved a sexual cyber-related violation.

In 2012, an accused was identified in 6% of property-related cybercrimes, 31% of sexual cyber-related violations, and 55% of cybercrimes related to intimidation violations. Compared to intimidation violations, sexual violations were more frequently cleared by the laying of a charge (25% versus 18%).

The majority (76%) of accused identified by police in 2012 were men. This finding was especially pronounced for violations of a sexual nature, where males accounted for 94% of accused identified by police.

In 2012, police identified 2,070 victims of violent incidents involving a cybercrime. Females accounted for the majority of victims of violent incidents associated with a cybercrime (69%), particularly when incidents involved a sexual violation (84%).

Victims of cybercrime identified by police tend to be young. In 2012, 42% of victims of police-reported cybercrime were under the age of 18. Almost all (96%) victims of sexual violations associated with a cybercrime were under the age of 18, including 10% of victims under the age of 12.

The majority of victims (73%) knew the accused. Victims of sexual violations involving a cybercrime were less likely to know the accused (57%) relative to victims of non-sexual violent violations (77%).

According to the 2009 General Social Survey, approximately 1.75 million persons aged 15 and over reported that they had been cyber-bullied. This represented 8% of Internet users aged 15 and over. Less than one in ten (7%) victims of cyber-bullying reported the incident to police.

Survey Descriptions

Uniform Crime Reporting Survey

This report uses data from the Incident-based Uniform Crime Reporting Survey (UCR2). The UCR2 is a microdata survey that captures detailed information on crimes reported to and substantiated by police, including the characteristics of victims, accused persons, and incidents. In response to changing information needs, the survey was modified in 2005 (UCR2.2) to enable the collection of criminal incidents related to hate crime, organized crime, and cybercrime.

The UCR 2.2 Survey collects information on incidents involving cyber-related violations. Incidents of crime may comprise multiple violations of the law. In 2012, there were 9,084 criminal incidents that included a violation that was identified as a cybercrime. For 8,974 (99%) of these incidents, the cyber-related violation was the most serious violation in the incident.

Data on police-reported cybercrime were available for police services representing 80% of the population of Canada. Data from Saint John, Québec, Toronto, Calgary, and the Ontario Provincial Police were not available and thus were not included in the present analysis.

General Social Survey on Victimization

In 2009, Statistics Canada conducted the victimization cycle of the General Social Survey (GSS) for the fifth time. Previous cycles were conducted in 1988, 1993, 1999 and 2004. The objectives of the survey are to provide estimates of Canadians' personal experiences of eight offence types, examine risk factors associated with victimization, examine rates of reporting to police, measure the nature and extent of spousal violence, measure fear of crime and examine public perceptions of crime and the criminal justice system. For the first time in 2009, the GSS also collected information on Canadians' experiences with victimization on the Internet, namely with Internet fraud, cyber-bullying, and problems making online purchases.

The target population included all persons 15 years and older in the 10 Canadian provinces, excluding full-time residents of institutions. Households were selected by telephone sampling using a random digit dialling method. Households that had no telephone or used a cell phone only were excluded. These two groups combined represented approximately 9% of the target population (Residential Telephone Service Survey, December 2008). Therefore, the coverage for 2009 was 91%. Data collection took place from February to November 2009 inclusively. From the 31,510 households that were selected for the

GSS Cycle 23 sample, 19,422 usable responses were obtained. This represents a response rate of 61.6%. Each person who responded to the 2009 GSS represented roughly 1,400 people in the Canadian population aged 15 years and over.

References

Brennan, Shannon. 2012. "Police-reported crime statistics in Canada, 2011." *Juristat*. Statistics Canada Catalogue no. 85-002-X.

Canadian Anti-Fraud Centre. 2014. "Annual Statistical Report 2013: Mass Marketing Fraud and ID Theft Activities." Canadian Anti-Fraud Centre Criminal Intelligence Analytical Unit. https://www.antifraudcentre-centreantifraude.ca/english/documents/Annual%202013%20CAFC.pdf (accessed September 8, 2014).

Canadian Centre for Justice Statistics. 2013. *Uniform Crime Reporting Incident-Based Survey Manual.* Unpublished.

Center for Strategic and International Studies. 2014. "Net Losses: Estimating the Global Cost of Cybercrime." Intel Security. http://www.mcafee.com/ca/resources/reports/rp-economics-impact-cybercrime2.pdf (accessed September 8, 2014).

Cotter, Adam and Pascale Beaupré. 2014. "Police-reported sexual offences against children and youth in Canada, 2012." *Juristat*. Statistics Canada Catalogue No. 85-002-X.

Cybertip.ca. 2014. Overall Statistics. http://www.cybertip.ca/app/en/about#about-our_results (accessed September 8, 2014).

Hotton Mahony, Tina and John Turner. 2012. "Police-reported clearance rates in Canada, 2010." *Juristat*. Statistics Canada Catalogue no. 85-002-X.

Kowalski, Melanie. 2002. "Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics." Canadian Centre for Justice Statistics. Statistics Canada Catalogue no. 85-558-X.

Norton. (2013). "2013 Norton Report." Symantec. http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.en_ca.pdf (accessed September 8, 2014).

Nuth, Maryke S. 2008. "Taking Advantage of New Technologies: For and Against Crime." *Computer Law and Security Review*. Vol. 24(5).

Perreault, Samuel. 2011. "Self-reported Internet victimization in Canada, 2009." *Juristat*. Statistics Canada Catalogue no. 85-002-X.

Perreault, Samuel. 2013. "Police-reported crime statistics in Canada, 2012." *Juristat*. Statistics Canada Catalogue no. 85-002-X.

Perreault, Samuel and Shannon Brennan. 2010. "Criminal victimization in Canada, 2009." *Juristat*. Statistics Canada Catalogue no. 85-002-X.

RCMP. 2014. "Cybercrime: An Overview of Incidents and Issues in Canada." *Royal Canadian Mounted Police*. Catalogue no. PS64-116/2014E-PDF. http://www.rcmp.grc.gc.ca/pubs/cc-report-rapport-cc-eng2.pdf (accessed September 8, 2014).

Smyth, Sara M. and Rebecca Carleton. 2011. "Measuring the Extent of Cyber-Fraud: A Discussion Paper on Potential Methods and Data Sources." Prepared for Research and National Coordination Organized Crime Division, Law Enforcement and Policing Branch, Public Safety Canada, No. 020,catalogue no. PS144/2011E-PDF. http://publications.gc.ca/collections/collection_2011/sp-ps/PS14-4-2011-eng.pdf (accessed September 8, 2014).

Statistics Canada. 2013. "Individual Internet use and E-commerce, 2012." *The Daily*. http://www.statcan.gc.ca/daily-quotidien/131028/dq131028a-eng.htm (accessed September 8, 2014).

Notes

1. The Incident-based Uniform Crime Reporting Survey (UCR2.2) captures detailed information on cybercrimes reported to and substantiated by police. For more information on the UCR2.2 survey, see 'Survey Descriptions.' For more information on the definition of incidents of cybercrime, see Text box 1.

2. For analytical purposes, incidents of cybercrime where the cyber-related violation was a non-*Criminal Code* offence have been excluded from the present report. As a result, 4 incidents of drug trafficking and 13 incidents related to other federal statute offences are excluded from this analysis.

3. Data on police-reported cybercrime were available for police services representing 80% of the population of Canada. Data from Saint John, Québec, Toronto, Calgary, and the Ontario Provincial Police were not available and thus were not included in the present analysis. For more information on the collection of police-reported cybercrime data, see Survey Descriptions.

4. Rate calculations are based on population counts derived from the subset of police services providing cybercrime data to the UCR2.2 survey.

5. The UCR violation '**Fraud**' is an aggregation of several *Criminal Code* offences. A fraud is a criminal act whereby an individual or group of individuals by deceit, falsehood or other fraudulent means, defrauds the public or any person, of any property, money, valuable security, or service. Any fraud that involves the unauthorized use of a computer or the use of a computer or the Internet for illegal means is a cybercrime. Identity fraud and identity theft are distinguished from fraud in the UCR survey.

6. This analysis only considers incidents of cybercrime substantiated by police, and therefore may not reflect all occurrences of online victimization experienced by Canadians. For a discussion of alternate data sources and estimations of cyber-fraud see Text box 4.

7. Violations against the person include sexual violations, intimidation violations, and other violent violations. Violations against the person include violations for which victim information either must be provided or is required if known. For the purposes of this analysis sexual violations include child pornography related offences, for which victim information is not available. For a list of what offences are included in 'sexual violations' and 'intimidation violations' respectively, see Table 1.

8. The UCR violation **'Luring a child/ Agreement or arrangement'** includes two separate *Criminal Code* offences: Luring a child via a computer (section 172.1) and Agreement or arrangement – sexual offence against child (section 172.2). Luring a child via a computer is a hybrid offence that criminalizes communicating with a child by any means of telecommunication to facilitate the commission of a sexual offence against the child. Agreement or arrangement is a hybrid offence that criminalizes agreeing or making an arrangement with a person by means of telecommunication to commit a sexual offence against a child. This offence was enacted in August 2012. For each of these offences, the maximum penalty is 10 years imprisonment if prosecuted by indictment and 18 months if prosecuted by summary conviction. Mandatory minimum penalties of one year apply if prosecuted by indictment and 90 days if prosecuted by summary conviction.

9. Due to the complexity of these cybercrimes, the data likely reflect the number of active or closed investigations for the year rather than the total number of incidents reported to police. The UCR violation "child pornography" includes offences under section 163.1 of the *Criminal Code* which makes it illegal to access, possess, make, print, or distribute child pornography. When the actual victim is not identified, this offence is reported to the Uniform Crime Reporting Survey with the most serious violation being "Child pornography." For the purposes of analyzing incidents of cybercrime, these violations are included with 'sexual violations', which are grouped under cybercrimes against the person. In cases where an actual victim is identified, police will report the most serious offence as sexual assault, sexual exploitation or other sexual violations against children, and child pornography may be reported as a secondary violation.

10. For an incident to be cleared, an accused must be identified and there must be enough evidence to lay a charge in connection with the incident. Incidents may be cleared by charge or processed by other means (i.e. cleared otherwise). Police-reported crime statistics have consistently shown that property related offences are less likely to be cleared as compared to violent violations (Hotton Mahony and Turner 2012).

11. Analysis of victims of police-reported cybercrime is based on victims of violent crimes that included a cyber-related violation within the same incident. Victims are categorized based upon the violation against the victim. The violation against the victim is not necessarily the cyber-related violation in the incident. There may be multiple victims associated with an incident of crime. It is possible that the number of victims analyzed in this report is an underestimation given that detailed victim information may not be available for particular violent violations, including luring a child via a computer, voyeurism, extortion, criminal harassment, and uttering threats. Further, victim information is only available for violent violations and

therefore persons who were the target of cybercrimes against property, such as fraud, are not considered in the analysis of victims.

12. For the purposes of analyzing victims of violent incidents associated with a cybercrime, the violation against the victim has been categorized as either a violent sexual violation or a non-sexual violent violation. See Table 5 for a list of which violations are included in the respective categories. Violent sexual violations do not include child pornography-related offences, as victim information is not available for this violation. See footnote 9 for an explanation of how child pornography offences are reported to the UCR Survey.

13. The proportion of victims victimized by a stranger may be an underestimation as some victims are not identified by police.

14. The most current data available from the General Social Survey on Victimization are results from 2009. For more analysis of self-reported Internet victimization in Canada based on results from the 2009 GSS, see Perreault, 2011. The GSS on Victimization is conducted every five years, with the 2014 survey cycle currently underway.

15. Previous research indicates that children and youth are at an increased risk of being the victim of cyber-bullying. Adult respondents to the 2009 GSS were asked if any of the children (aged 8 to 17) in their household had been the victim of cyber-bullying. Approximately one in ten adults living in a household that included a child knew of a case of cyber-bullying against at least one of the children in their household (Perreault 2011).

16. These percentages are based on whether or not a person was a victim of cyber-bullying. It is possible that these persons were victims of other types of crime.

17. For a list of daily cautions see Table 7.

Detailed data tables

Table 1
Police-reported cybercrimes, selected police services, 2012

Cyber-related violation[1]	Number	Rate per 100,000 population	Percentage of total
Total cybercrimes against the person	**3,284**	**11.8**	**36.2**
Sexual violations	**1,441**	**5.2**	**15.9**
Invitation to sexual touching	67	0.2	0.7
Sexual exploitation	10	0.0	0.1
Luring a child/ Agreement or arrangement	543	2.0	6.0
Voyeurism	11	0.0	0.1
Other sexual violations[2]	5	0.0	0.1
Child pornography[3]	805	2.9	8.9
Intimidation violations	**1,839**	**6.6**	**20.2**
Extortion	136	0.5	1.5
Intimidation of an individual[4]	7	0.0	0.1
Criminal harassment	560	2.0	6.2
Threatening or harassing phone calls	377	1.4	4.2
Uttering threats	759	2.7	8.4
Other violent violations[5]	**4**	**0.0**	**0.0**
Total cybercrimes against property	**5,544**	**20.0**	**61.0**
Fraud	4,878	17.6	53.7
Identity theft	73	0.3	0.8
Identity fraud	421	1.5	4.6
Mischief	170	0.6	1.9
Trafficking stolen goods	2	0.0	0.0
Total other *Criminal Code* violations[6]	**256**	**0.9**	**2.8**
Total - all *Criminal Code* violations	**9,084**	**32.7**	**100.0**

1. Counts are based upon the violation in the incident where a computer or the Internet was the target of the crime or the instrument used to commit the crime.
2. Other sexual violations include corrupting children, making sexually explicit material available to children, and bestiality - commit or compel person.
3. Due to the complexity of these cybercrimes, the data likely reflect the number of active or closed investigations for the year rather than the total number of incidents reported to police. The violation "child pornography" includes offences under section 163.1 of the *Criminal Code* which makes it illegal to access, possess, make, print, or distribute child pornography. When the actual victim is not identified, this offence is reported to the Uniform Crime Reporting Survey with the most serious violation being "Child pornography." For the purposes of this analysis, these violations are included with 'sexual violations', which are grouped under cybercrimes against the person. In cases where an actual victim is identified, police will report the most serious violation as sexual assault, sexual exploitation or other sexual violations against children, and child pornography may be reported as a secondary violation.
4. Intimidation of an individual includes intimidation of a justice system participant or journalist and intimidation of a non-justice system participant.
5. Other violent violations include trafficking in persons and other violent violations.
6. Other *Criminal Code* violations include offences such as corrupting morals, indecent acts, offences against the person and reputation, fail to comply with order, and breach of probation.

Note: This table reflects data reported by police services covering 80% of the population of Canada. Data from Saint John, Québec City, Toronto, Calgary, and the Ontario Provincial Police were not available and thus were not included in the present analysis.
Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

Table 2
Police-reported cybercrimes, by clearance status, selected police services, 2012

Cyber-related violation[1]	Cleared by charge		Cleared otherwise		Not cleared		Total
	number	percent	number	percent	number	percent	number
Total cybercrimes against the person	**697**	**21.2**	**762**	**23.2**	**1,825**	**55.6**	**3,284**
Sexual violations	**357**	**24.8**	**92**	**6.4**	**992**	**68.8**	**1,441**
Invitation to sexual touching	53	79.1	2	3.0	12	17.9	67
Sexual exploitation	5	50.0	2	20.0	3	30.0	10
Luring a child/ Agreement or arrangement	146	26.9	41	7.6	356	65.6	543
Voyeurism	8	72.7	2	18.2	1	9.1	11
Other sexual violations[2]	1	20.0	0	0.0	4	80.0	5
Child pornography[3]	144	17.9	45	5.6	616	76.5	805
Intimidation violations	**339**	**18.4**	**667**	**36.3**	**833**	**45.3**	**1,839**
Extortion	23	16.9	14	10.3	99	72.8	136
Intimidation of an individual[4]	1	14.3	1	14.3	5	71.4	7
Criminal harassment	200	35.7	193	34.5	167	29.8	560
Threatening or harassing phone calls	9	2.4	154	40.8	214	56.8	377
Uttering threats	106	14.0	305	40.2	348	45.8	759
Other violent violations[5]	**1**	**25.0**	**3**	**75.0**	**0**	**0.0**	**4**
Total cybercrimes against property	**144**	**2.6**	**212**	**3.8**	**5,188**	**93.6**	**5,544**
Fraud	126	2.6	115	2.4	4,637	95.1	4,878
Identity theft	0	0.0	2	2.7	71	97.3	73
Identity fraud	8	1.9	71	16.9	342	81.2	421
Mischief	8	4.7	24	14.1	138	81.2	170
Trafficking stolen goods	2	100.0	0	0.0	0	0.0	2
Total other *Criminal Code* violations[6]	**66**	**25.8**	**49**	**19.1**	**141**	**55.1**	**256**
Total - all *Criminal Code* violations	**907**	**10.0**	**1,023**	**11.3**	**7,154**	**78.8**	**9,084**

1. Counts are based upon the violation in the incident where a computer or the Internet was the target of the crime or the instrument used to commit the crime. For an incident to be cleared an accused must be identified and there must be enough evidence to lay a charge in connection with the incident. Incidents may be cleared by charge or processed by other means (i.e. cleared otherwise).
2. Other sexual violations include corrupting children, making sexually explicit material available to children, and bestiality - commit or compel person.
3. Due to the complexity of these cybercrimes, the data likely reflect the number of active or closed investigations for the year rather than the total number of incidents reported to police. The violation "child pornography" includes offences under section 163.1 of the *Criminal Code* which makes it illegal to access, possess, make, print, or distribute child pornography. When the actual victim is not identified, this offence is reported to the Uniform Crime Reporting Survey with the most serious violation being "Child pornography." For the purposes of this analysis, these violations are included with 'sexual violations', which are grouped under cybercrimes against the person. In cases where an actual victim is identified, police will report the most serious violation as sexual assault, sexual exploitation or other sexual violations against children, and child pornography may be reported as a secondary violation.
4. Intimidation of an individual includes intimidation of a justice system participant or journalist and intimidation of a non-justice system participant.
5. Other violent violations include trafficking in persons and other violent violations.
6. Other *Criminal Code* violations include offences such as corrupting morals, indecent acts, offences against the person and reputation, fail to comply with order, and breach of probation.

Note: This table reflects data reported by police services covering 80% of the population of Canada. Data from Saint John, Québec City, Toronto, Calgary, and the Ontario Provincial Police were not available and thus were not included in the present analysis.
Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

Table 3
Characteristics of persons accused of police-reported cybercrime, by cyber-related violation, selected police services, 2012

Demographics[1,2]	Total cybercrimes against the person[3]		Sexual violations[4]		Intimidation violations		Total cybercrimes against property[5]		Total other *Criminal Code* violations[6]		Total - all *Criminal Code* violations	
	number	%	number	%	number	%	number	%	number	%	number	%
Sex												
Female	367	23.5	29	6.1	333	30.9	99	26.6	29	24.8	495	24.1
Male	1,195	76.5	450	93.9	743	69.1	273	73.4	88	75.2	1,556	75.9
Total	**1,562**	**100**	**479**	**100**	**1,076**	**100**	**372**	**100**	**117**	**100**	**2,051**	**100**
Age												
Under 12 years	12	0.8	1	0.2	11	1.0	1	0.3	0	0.0	13	0.6
12 to 17 years	371	23.8	75	15.7	290	27.0	35	9.4	18	15.4	424	20.7
18 to 24 years	324	20.7	90	18.8	234	21.7	90	24.2	18	15.4	432	21.1
25 to 34 years	335	21.4	107	22.3	227	21.1	154	41.4	36	30.8	525	25.6
35 to 44 years	262	16.8	84	17.5	178	16.5	61	16.4	29	24.8	352	17.2
45 to 54 years	178	11.4	76	15.9	102	9.5	23	6.2	12	10.3	213	10.4
55 years and over	80	5.1	46	9.6	34	3.2	8	2.2	4	3.4	92	4.5
Total	**1,562**	**100**	**479**	**100**	**1,076**	**100**	**372**	**100**	**117**	**100**	**2,051**	**100**

1. Accused counts are based upon the cyber-related violation within the incident.
2. Accused records with unknown age or sex are excluded.
3. Total cybercrimes against the person include sexual violations against the person, child pornography related offences, intimidation violations involving the threat of violence, and other violent violations.
4. Sexual violations include sexual violations against the person and child pornography related offences.
5. Total cybercrimes against property includes fraud, identity theft, identity fraud, mischief and trafficking stolen goods.
6. Other *Criminal Code* violations include offences such as corrupting morals, indecent acts, offences against the person and reputation, fail to comply with order, and breach of probation.

Note: This table reflects data reported by police services covering 80% of the population of Canada. Data from Saint John, Québec City, Toronto, Calgary, and the Ontario Provincial Police were not available and thus were not included in the present analysis.
Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

Table 4
Characteristics of police-reported cybercrime victims, by the violation against the victim, selected police services, 2012

Demographics[1,2]	Total violent violations		Sexual violations[3]		Non-sexual violent violations[4]	
	number	percentage	number	percentage	number	percentage
Sex						
Female	1,432	69.2	394	84.2	1,038	64.8
Male	638	30.8	74	15.8	564	35.2
Total	**2,070**	**100**	**468**	**100**	**1,602**	**100**
Age						
Under 12 years	82	4.0	49	10.5	33	2.1
12 to 17 years	785	37.9	401	85.7	384	24.0
18 to 24 years	355	17.1	7	1.5	348	21.7
25 to 34 years	317	15.3	7	1.5	310	19.4
35 to 44 years	275	13.3	4	0.9	271	16.9
45 to 54 years	167	8.1	0	0.0	167	10.4
55 years and over	89	4.3	0	0.0	89	5.6
Total	**2,070**	**100**	**468**	**100**	**1,602**	**100**

1. Counts are based upon the violation against the victim, which is not necessarily the cyber-related violation in the incident.
2. Victim records with unknown age or sex are excluded.
3. Sexual violations include sexual assaults, sexual interference, invitation to sexual touching, luring a child via a computer, and other sexual violations against the person.
4. Non-sexual violent violations include assaults, extortion, criminal harassment, threatening or harassing phone calls, uttering threats, and other non-sexual violent violations.

Note: This table reflects data reported by police services covering 80% of the population of Canada. Data from Saint John, Québec City, Toronto, Calgary, and the Ontario Provincial Police were not available and thus were not included in the present analysis.
Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

Table 5
Police-reported victims of violent violations associated with a cybercrime, by relationship of the accused to the victim, selected police services, 2012

	Relationship of the accused to the victim										
	Intimate partner[3]		Family member		Friend or acquaintance[4]		Stranger		Unknown[5]		Total
Violation against the victim[1,2]	number	%	number	%	number	%	number	%	number	%	number
Total violent crimes	**448**	**23.7**	**90**	**4.8**	**843**	**44.5**	**512**	**27.0**	**177**	**...**	**2,070**
Sexual violations	**35**	**8.7**	**15**	**3.7**	**181**	**44.9**	**172**	**42.7**	**65**	**...**	**468**
Sexual assault with a weapon or causing bodily harm (level 2)	0	0.0	0	0.0	1	100.0	0	0.0	0	...	1
Sexual assault (level 1)	18	29.5	8	13.1	32	52.5	3	4.9	6	...	67
Sexual interference	4	21.1	3	15.8	12	63.2	0	0.0	0	...	19
Invitation to sexual touching	1	2.1	1	2.1	24	51.1	21	44.7	1	...	48
Sexual exploitation	1	11.1	0	0.0	7	77.8	1	11.1	1	...	10
Luring a child/ Agreement or arrangement	10	3.9	3	1.2	101	39.5	142	55.5	56	...	312
Voyeurism	1	14.3	0	0.0	4	57.1	2	28.6	0	...	7
Other sexual violations[6]	0	0.0	0	0.0	0	0.0	3	100.0	1	...	4
Non-sexual violent violations	**413**	**27.7**	**75**	**5.0**	**662**	**44.4**	**340**	**22.8**	**112**	**...**	**1,602**
Aggravated assault (level 3)	1	50.0	0	0.0	1	50.0	0	0.0	0	...	2
Assault with a weapon or causing bodily harm (level 2)	7	70.0	0	0.0	1	10.0	2	20.0	1	...	11
Assault (level 1)	8	47.1	0	0.0	8	47.1	1	5.9	0	...	17
Extortion	16	18.0	1	1.1	19	21.3	53	59.6	14	...	103
Intimidation of an individual[7]	2	25.0	0	0.0	3	37.5	3	37.5	0	...	8
Criminal harassment	213	47.3	21	4.7	169	37.6	47	10.4	23	...	473
Threatening or harassing phone calls	76	26.4	8	2.8	128	44.4	76	26.4	14	...	302
Uttering threats	88	14.3	42	6.8	328	53.4	156	25.4	59	...	673
Other violent violations[8]	2	16.7	3	25.0	5	41.7	2	16.7	1	...	13

... not applicable
1. Counts are based upon the violation against the victim, which is not necessarily the cyber-related violation in the incident.
2. Victim records with unknown age or sex are excluded.
3. Intimate partner includes current or former spouses, current or former dating relationships, and other intimate relationships.
4. Friend or acquaintance includes friends, casual acquaintances, neighbours, business relationships, criminal relationships and authority figures.
5. Unknowns are excluded from percentage calculations.
6. Other sexual violations include corrupting children, making sexually explicit material available to children, and bestiality - commit or compel person.
7. Intimidation of an individual includes intimidation of a justice system participant or journalist and intimidation of a non-justice system participant.
8. Other violent violations include forcible confinement or kidnapping, abduction, trafficking in persons, robbery, and other violent violations.
Note: This table reflects data reported by police services covering 80% of the population of Canada. Data from Saint John, Québec City, Toronto, Calgary, and the Ontario Provincial Police were not available and thus they are not included in the present analysis.
Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

Table 6
Self-reported victims of cyber-bullying, by the sex and age of victims, Canada, 2009

	Cyber-bullying victims	
Demographics	number (thousands)	percentage
Sex		
Female†	899	8
Male	866	8
Age group		
15 to 17 years†	270	19
18 to 24 years	527	17
25 to 34 years	388	9*
35 to 44 years	228	5*
45 to 54 years	221	5*
55 years and over	130	3*
Incidents reported to the police	116	7
Total	**1,765**	**8**

† reference group
* significantly different from reference category ($p < 0.05$)
Note: Includes respondents aged 15 years and over. Respondents were asked if they had ever been the victim of cyber-bullying. As such, there is no time period for cyber-bullying. Percentage calculations are based upon all Canadians who used the Internet at least once during the 12 months preceding the survey.
Source: Statistics Canada, General Social Survey, 2009.

Table 7
Self-reported victims of cyber-bullying, by protective measures and daily caution taken, Canada, 2009

	Victims of cyber-bullying, by whether or not they were also a victim of a violent crime				Totals for victims and non-victims of cyber-bullying	
	Victims of cyber-bullying only	Victims of cyber-bullying and a violent crime	Not a victim of cyber-bullying, but a victim of a violent crime	Not of victim of cyber-bullying or a violent crime†	Victims of cyber-bullying	Not a victim of cyber-bullying†
Safety caution used	percentage					
At least one new protection has been taken during the last 12 months	54*	75*	64*	39	59*	40
New protection type taken during the last 12 months						
Changing the routine, activities, or avoiding certain people or places	42*	66*	50*	26	47*	28
Installing new locks or security bars	15	30*	24*	13	18*	13
Installing burglar alarms or motion detector lights	13	13[E]	13*	10	13	11
Taking a self-defence course	5*[E]	10*[E]	8*	2	6*	3
Obtaining a dog	4[E]	8*[E]	5*	2	5[E]*	3
Obtaining a gun	F	F	F	0	F	0
Changing residence or moving	2[E]	6*[E]	4*[E]	1	3[E]*	1
Daily caution taken						
Carrying something to defend yourself or to alert other people	25*	39*	30*	13	28*	15
Checking the back seat for intruders before getting into a vehicle when alone	44	48	46*	40	45*	40
Planning your route with safety in mind	51*	60*	51*	43	53*	43
Staying at home at night because the respondent is afraid to go out alone	12	20*[E]	11	8	14*	8
Locking windows and doors at home	85	87	85	85	86	85
Rather than walking, using the car, a taxi, or public transportation for personal safety	36*	54*	40*	31	40*	31
Other safety precautions	16	27*[E]	21*	14	19*	14
	number (thousands)					
Total	**1,386**	**378**	**1,331**	**19,720**	**1,765**	**21,051**

E use with caution
F too unreliable to be published
† reference group
* significantly different from reference category ($p < 0.05$)
Note: Includes respondents aged 15 years and over. Percentage calculations are based upon all Canadians who used the Internet at least once during the 12 months preceding the survey. Respondents were asked if they had ever been the victim of cyber-bullying. As such, there is no time period for cyber-bullying. Respondents were asked about their daily safety precautions taken in an unspecified length of time. As a result, precautions may be new or habitual.
Source: Statistics Canada, General Social Survey, 2009.